AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method comprising:

reading from a software module binary a set of keys associated with a trusted source, wherein the set of keys is embedded in the software module binary, the set of keys having been compiled and linked with a software module to generate the software module binary;

determining whether a key is traceable to one of the keys in the set of keys, the key being presented by or read from a document comprising a digital signature of the software module binary;

determining whether the key is identified in a list of compromised keys; and

if the key is not identified as compromised and is traceable to one of the keys in the set of keys, assigning the key a trusted status.

2. (Previously Presented) The method of claim 1 further comprising:

verifying the integrity of the document, the document further comprising the list of compromised keys.

3. (Cancelled).

4. (Previously Presented) The method of claim 1 in which determining whether the key is traceable to one of the keys in the set of keys further comprises:

tracing the key through a certificate chain to one of the keys in the set of keys.

5. (Previously Presented) The method of claim 1 wherein the digital signature is a hash of the software module binary.

6. (Original) The method of claim 2 in which the document is a manifest signed by the key.

7. (Original) The method of claim 1 in which determining whether the key is identified in the list of compromised keys further comprises:

searching the list of compromised keys for the key.

8. (Currently Amended) A method comprising:

producing a document comprising an identification of a software module binary and a list of compromised keys; ~~and~~

digitally signing the document using a key presented by or read from the document and traceable to one key of a set of keys, wherein the set of keys is embedded in the software module binary, the set of keys having been compiled and linked with a software module to generate the software module binary;~~.~~ and

making the document available on a communication network by which computer systems comprising the software module binary may read the document.

9. (Previously Presented) The method of claim 8 in which the identification of the software module binary comprises a hash value of the software module binary.

10. (Previously Presented) The method of claim 8 in which the key is traceable to one of the keys in the set of keys embedded in the software module binary by way of a certificate chain.

11. (Cancelled)

12. (Cancelled).

13. (Previously Presented) A device comprising:

a processor;

a machine-readable storage medium coupled to the processor by way of a bus, the storage medium storing instructions which, when executed by the processor, cause the device to

read from a software module binary a set of keys associated with a trusted source, wherein the set of keys is embedded in the software module binary, the set of keys having

been compiled and linked with a software module to generate the software module binary,

determine whether a key is traceable to one of the keys in the set of keys, the key being presented by or read from a document comprising a digital signature of the software module binary,

determine whether the key is identified in a list of compromised keys, and

if the key is not identified as compromised and is traceable to one of the keys in the set of keys, assign the key a trusted status.

14. (Previously Presented) The device of claim 13 in which the instructions, when executed by the device, further cause the device to:

verify the integrity of the document, the document further comprising the list of compromised keys.

15. (Canceled)

16. (Previously Presented) The device of claim 13 in which the instructions, when executed by the device, further cause the device to:

trace the key through a certificate chain to one of the keys in the set of keys.

17. (Currently Amended) A device comprising:

a processor;

a machine-readable storage medium coupled to the processor by way of a bus, the storage medium storing instructions which, when executed by the processor, cause the device to:

produce a document comprising an identification of a software module binary and a list of compromised keys; and

digitally sign the document using a key presented by or read from the document and traceable to one key of a set of keys, wherein the set of keys is embedded in the

software module binary, the set of keys having been compiled and linked with a software module to generate the software module binary~~;~~,

wherein the key is traceable to one of the keys in the set of keys embedded in the software module binary by way of a certificate chain.

18. (Previously Presented) The device of claim 17 in which the identification of the software module binary comprises a hash value of the software module binary.

19. (Cancelled)

20. (Previously Presented) An article comprising a machine-readable medium having stored thereon instructions which, when executed by a processor, result in:

reading from a software module binary a set of keys associated with a trusted source, wherein the set of keys is embedded in the software module binary, the set of keys having been compiled and linked with a software module to generate the software module binary;

determining whether a key is traceable to one of the keys in the set of keys, the key being presented by or read from a document comprising a digital signature of the software module binary;

determining whether the key is identified in a list of compromised keys; and

if the key is not identified as compromised and is traceable to one of keys in the set of keys, assigning the key a trusted status.

21. (Previously Presented) The article of claim 20 in which the instructions, when executed by the processor, further result in:

verifying the integrity of the document, the document further comprising the list of compromised keys.

22. (Cancelled).

23. (Previously Presented) The article of claim 20 in which the sequence of instructions, when executed by the processor, further result in:

tracing the key through a certificate chain to one of the keys in the set of keys.

24. (Currently Amended) An article comprising a machine-readable medium having stored thereon instructions which, when executed by a processor, result in:

producing a document comprising an identification of a software module binary and a list of compromised keys; and

digitally signing the document using a key presented by or read from the document and traceable to one key of a set of keys, wherein the set of keys is embedded in the software module binary, the set of keys having been compiled and linked with a software module to generate the software module binary~~.~~;

wherein the identification of the software module binary comprises a hash value of the software module binary.

25. (Cancelled)

26. (Previously Presented) The article of claim 24 in which the key is traceable by way of a certificate chain to one of the keys in the set of keys embedded in the software module binary.